Requestor has appealed the denial by the City of Harrisburg Police Department to produce "any/all manuals regarding CRIMEWATCH Technologies products/services". In fact, the manuals requested in this Appeal are exempt from disclosure under exemptions contained within the Pennsylvania Right-to-Know Law ("RTKL"), 65 P.S. §67.101, et seq.

Trade Secret and Confidential Proprietary Information Exemption, 65 P.S. §67.708(b)(11).

1. Trade Secrets.

The RTKL provides that a "record that constitutes or reveals a trade secret or confidential proprietary information" is exempt from disclosure. 65 P.S. §67.708(b)(11). The RTKL defines "trade secret" as:

> Information, including a formula, drawing, pattern, compilation, including a customer list, program, device, method, technique or process that: (1) derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

65 P.S. §67.102. This definition is identical to that contained in Pennsylvania's Uniform Trade Secrets Act, 12 P.S. §5302, 5308.

The Commonwealth Court has held that information may constitute a "trade secret" based upon various factors:

> (1) the extent to which the information is known outside of the business; (2) the extent to which the information is known by employees and others in the business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of the information to the business and to competitors; (5) the amount of effort or money expended in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Smith ex rel. Smith Butz, LLC v. DEP, 161 A.3d 1049 (Pa. Commw. 2017) (citations omitted). Moreover, a "trade secret" "must be an 'actual secret of peculiar importance to the business and constitute competitive value to the owner.'" Parsons v. Pennsylvania Higher Education Assistance Agency, 910 A.2d 177, 185 (Pa. Commw. 2006). "The most critical criteria are 'substantial secrecy and competitive value.'" Commonwealth v. Eiseman, 85 A.3d 1117, 1126 (Pa. Commw. 2014), *quoting* Crum v. Bridgestone/Firestone North American Tire, 907 A.2d 578, 585 (Pa. Super. 2006).

In this case, the requested manuals of CRIMEWATCH Technologies, Inc. ("CRIMEWATCH") contain information that constitute programs, software, techniques and processes that derive independent economic value from not being generally known to and not being readily ascertainable by proper means by other persons, and this information is subject to substantial efforts by CRIMEWATCH to maintain the secrecy thereof.

CRIMEWATCH was specifically designed to assist law enforcement agencies. As stated in the accompanying Affidavit of CRIMEWATCH Chief Technology Officer Mike Grucz, CRIMEWATCH training/user manuals are all embedded and integrated directly into the CRIMEWATCH technology platform and releasing these would disclose proprietary design and function of the CRIMEWATCH platform. In that regard, there are no hard copies of any CRIMEWATCH training and user manuals; users can only get quick reference cards with paid access to the entire platform itself, but those quick reference cards would contain screenshots and URL/Web Addresses containing sensitive customer-only URLs. Thus, releasing training/user manuals to the public would expose sensitive customer-only URLs throughout the CRIMEWATCH Network. Grucz Affidavit, page 1-2.

Moreover, public disclosure of these embedded and integrated materials would expose highly customized content types, workflows, and processes to competitors, as well as CRIMEWATCH's trademarked ControlShare ™ technology, thereby opening a door to reverse engineering or cloning of CRIMEWATCH's highly matured and refined software and trademarked intellectual property. Hackers are also a concern, and "[a]rming them with details as to how to curate and pull together content on [CRIMEWATCH's] government/Law Enforcement customer portals means they now know which fields are required when creating various content types." Grucz Affidavit, page 2-4.

It should be noted that Section 705 of the RTKL provides that "[w]hen responding to a request for access, an agency shall not be required to create a record which does not currently exist or to compile, maintain, format or organize a record in a manner in which the agency does not currently compile, maintain, format or organize the record." 65 P.S. §67.705. In this case, the Agency does not have access to any quick reference cards, so it would have to produce the entire CRIMEWATCH confidential and proprietary platform. *See* Grucz Affidavit, page 2. CRIMEWATCH and the Agency should not have to provide information that is embedded and integrated directly into the CRIMEWATCH platform and not maintained in hard copy form.

The requested information is highly valuable to CRIMEWATCH and (would be) to its many industry competitors, including Neighbors App by RING (Amazon); NextDoor for Public Safety; Citizen App; Nixle by EverBridge; and others. CRIMEWATCH and its owner, Matthew W. Bloom, spent nearly 11 years and over two million dollars to develop the CRIMEWATCH product and the information, software and technology that comprises the platform under which CRIMEWATCH conducts business operations. Grucz Affidavit, pages 2-4.

On the issue of security measures, the Grucz Affidavit states that:

> Only contracted police departments and authorized police department users, following CJIS (Criminal Justice Information Standards) with

> CLEAN[1] certified are given access to these training tools and any corresponding documentation. All of this access is controlled through a Point of Contact at each department and is subject to regular audits. Each authorized user's activity is then monitored through a separate security application. The training program is provided through an access token to each authorized user and expires within 30 days. This access is monitored electronically as well. Every authorized user has to successfully complete the training program before they are granted full access to the platform. During this time, they can download quick reference cards, but this is done so with the expectation that they are not shared outside of the organization with non-authorized users. Being that our customers are police departments, integrity in these processes are of high importance as they are regulated throughout the organization.

Grucz Affidavit, page 3. CRIMEWATCH only shares its embedded and integrated training/user manuals with law enforcement customers to whom CRIMEWATCH provides contracted services, and police department users follow CJIS standards and must be CLEAN certified, subject to regular audits and monitoring.

Moreover, CRIMEWATCH employees only know the CRIMEWATCH product and the proprietary interfaces that drive its proprietary system on a "need-to-know" basis. Sales and marketing have a more rudimentary understanding while customer service representatives have a higher level of understanding. However, "[o]nly the development team has full access to the proprietary nature of the engineering and processes happening throughout the system. These employees are subject to an inventions assignment and non-disclosure agreements, as are all employees of CRIMEWATCH." Grucz Affidavit, page 3.

The requested materials are actual secrets of particular importance to CRIMEWATCH and constitute competitive value to CRIMEWATCH. Moreover, releasing these materials would be economically damaging to CRIMEWATCH because the platform could be cloned and used to diminish CRIMEWATCH's market presence. *See* Grucz Affidavit. Based on the foregoing, the embedded and integrated training/user manuals are exempt as trade secrets under 65 P.S. §67.708(b)(11) of the RTKL and the Pennsylvania Uniform Trade Secrets Act. *See* 12 P.S. §5302, 5308. See also Smith ex rel. Smith Butz, LLC v. DEP, 161 A.3d 1049 (Pa. Commw. 2017) (citations omitted).

---

[1] "CLEAN" refers to the Commonwealth Law Enforcement Assistance Network, which is a background verification that all members of law enforcement must have in order to access criminal justice systems in Pennsylvania. Anyone touching a computer in a police department must have a CLEAN certification because security and network integrity are of critical importance to law enforcement.

2. Confidential Proprietary Information.

The RTKL also exempts "confidential proprietary information". 65 P.S. §67.708(b)(11). This term is defined as "[c]ommercial or financial information received by an agency: (1) which is privileged or confidential; and (2) the disclosure of which would cause substantial harm to the competitive position of the person that submitted the information." 65 P.S. §67.102. *See* Giurintano v. Department of General Services, 20 A.3d 613, 615-616 (Pa. Commw. 2011).

The Commonwealth Court has held that in determining whether information is "confidential," the Office of Open Records must consider "the efforts the parties undertook to maintain their [sic] secrecy." Commonwealth v. Eiseman, 85 A.3d 1117, 1128 (Pa. Commw. 2014), "In determining whether disclosure of confidential information will cause 'substantial harm to the competitive position' of the person from whom the information was obtained, an entity needs to show: (1) actual competition in the relevant market; and, (2) a likelihood of substantial injury if the information were released." Id. In addition, "[c]ompetitive harm analysis 'is limited to harm flowing from the affirmative use of proprietary information by competitors . . . . " Id., *citing* Watkins v. United States Bureau of Customs, 643 F.3d 1189, 1194 (9th Cir. 2011).

The requested manuals, provided to the City of Harrisburg Police Department as a paid law enforcement customer of CRIMEWATCH, are confidential to CRIMEWATCH's business. As stated, "only contracted police departments and authorized police department users, following CJIS (Criminal Justice Information Standards) with CLEAN certified are given access to these training tools and any corresponding documentation. All of this access is controlled through a Point of Contact at each department and is subject to regular audits. Each authorized user's activity is then monitored through a separate security application." Grucz Affidavit, page 3.

CRIMEWATCH reiterates that its embedded and integrated training/user manuals are only shared with law enforcement customers to whom CRIMEWATCH provides contracted services, and police department users follow CJIS standards and must be CLEAN certified, subject to regular audits and monitoring. Employees are provided proprietary information on a "need-to-know" basis and "[o]nly the [CRIMEWATCH] development team has full access to the proprietary nature of the engineering and processes happening throughout the system. These employees are subject to an inventions assignment and non-disclosure agreements, as are all employees of CRIMEWATCH." Grucz Affidavit, page 3. Thus, CRIMEWATCH has undertaken substantial efforts to maintain the secrecy of its information, including training and user manuals embedded and integrated into the CRIMEWATCH platform.

Moreover, there is actual competition in the relevant market. CRIMEWATCH has numerous competitors in the markets it serves. These include Neighbors App by RING (Amazon); NextDoor for Public Safety; Citizen App; Nixle by EverBridge; and possibly Harris Computer Systems who CRIMEWATCH believes is trying to create a competitive product. Grucz Affidavit, page 1.

There is also a likelihood of substantial injury to CRIMEWATCH if the information were released to the public. The Grucz Affidavit reveals that CRIMEWATCH's embedded and integrated training and user materials are solely for paying customers and would contain

screenshots that include URL/Web Addresses. Releasing training/user manuals to the public would, therefore, expose sensitive customer-only URLs throughout the CRIMEWATCH Network. Moreover, public disclosure of these materials would expose highly customized content types, workflows, and processes to competitors, as well as CRIMEWATCH's trademarked ControlShare ™ technology, thereby opening a door to reverse engineering or cloning of CRIMEWATCH's highly matured and refined software and trademarked intellectual property. *See* Grucz Affidavit, page 2.

This information is highly valuable to CRIMEWATCH and to its many competitors named hereinabove. CRIMEWATCH and its owner, Matthew W. Bloom, spent nearly 11 years and more than 2 million dollars to develop the CRIMEWATCH product and the information and technology that comprises the platform under which CRIMEWATCH conducts business operations. Based on the foregoing, CRIMEWATCH's proprietary training/user manuals are exempt "confidential proprietary information" under the RTKL.

Computer Security, 65 P.S. §67.708(b)(4).

The RTKL provides that a "record regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security" is exempt from disclosure. 65 P.S. §67.708(b)(4).

In this case, CRIMEWATCH's CTO has stated that "disclosure of the CRIMEWATCH training material would expose critical details of the CRIMEWATCH infrastructure that would increase the likelihood of cyber-attack and create catastrophic threats to the content delivery network which includes, the web, mobile, social applications and the private broadcast network of TVs." Grucz Affidavit, page 3. See also page 2 relating to domestic and foreign hackers.

Accordingly, public release of the embedded and integrated CRIMEWATCH training/user manuals would be reasonably likely to jeopardize computer security and CRIMEWATCH's content delivery network, thereby affecting law enforcement activities. As such, the requested material should be exempt under §67.708(b)(4) of the RTKL.

Conclusion.

CRIMEWATCH works hand in hand with law enforcement and provides a valuable tool benefitting both police departments and the public. Through the CRIMEWATCH web portal, citizens can access public safety information as well as share valuable information to law enforcement agencies; numerous crimes have been solved using information submitted through the CRIMEWATCH web portal. If the requested confidential and proprietary documents were shared with the public at large, it would be easy to duplicate the efforts that took nearly eleven years and millions of dollars to develop. This disclosure would provide a roadmap of where to start when duplicating the system and would cause substantial harm to the competitive position of CRIMEWATCH.

Under the circumstances, CRIMEWATCH respectfully requests that the Appeal of J. Ader be denied.

Respectfully submitted,
BENNLAW**FIRM**

By: _____

Terence J. Barna, Esquire
Attorney I.D. #74410
103 E. Market Street
P.O. Box 5185
York, PA 17405-5185
Phone: (717) 852-7020
Fax: (717) 852-8797
tbarna@bennlawfirm.com